ECM3704 - NUMBER THEORY 2016-17

EXERCISE SHEET 3 (ASSESSED)

Please hand in your solutions to the starred questions via BART by 12 noon on Monday 5th December 2016.

10 marks out of 100 will be for presentation (reasoning clearly expressed, correct use of notation, etc.) Please consult the *Guide to Basic Study Skills* available on ELE.

1. Find all solutions (if there are any) to each of the following congruences:
   (i)* $x^2 \equiv -5 \pmod{7^3}$; **[5]**
   (ii)* $x^2 \equiv 3 \pmod{7^3}$; **[3]**
   (iii)* $x^2 + x + 7 \equiv 0 \pmod{81}$; **[7]**
   (iv) $x^3 + x^2 + 8 \equiv 0 \pmod{11^3}$.

Total for question: [15]

2. Using a primitive root of 19, or otherwise, find all solutions of the following congruences:
   (i) $x^5 \equiv 7 \pmod{19}$;
   (ii) $x^4 \equiv 4 \pmod{19}$;
   (iii)* $x^{10} \equiv 9 \pmod{19}$. **[5]**

Total for question: [5]

3. Let $n \in \mathbb{N}$ with $n \geq 2$. Show that if there is a primitive root mod n then in fact there exist exactly $\varphi(\varphi(n))$ incongruent primitive roots mod n.

4*. Prove that if p is a prime then there exist $\varphi(\varphi(p^2)) = (p-1)\varphi(p-1)$ primitive roots modulo p^2. **[15]**

Total for question: [15]

5*. Let p be a prime number. Prove that

$$\frac{(np)!}{n!p^n} \equiv (-1)^n \pmod{p}$$

[10]

Total for question: [10]

6. Evaluate each of the following Legendre symbols using quadratic reciprocity. (The numbers underneath are all primes.)

(i)* $\left(\frac{3}{53}\right)$; (ii) $\left(\frac{7}{79}\right)$; (iii)* $\left(\frac{15}{101}\right)$; (iv) $\left(\frac{31}{641}\right)$;
(v) $\left(\frac{111}{991}\right)$; (vi) $\left(\frac{105}{1009}\right)$; (vii) $\left(\frac{77}{107}\right)$; (viii)* $\left(\frac{133}{191}\right)$;
(ix)* $\left(\frac{-111}{257}\right)$; (x) $\left(\frac{221}{347}\right)$; (xi)* $\left(\frac{-257}{541}\right)$; (xii) $\left(\frac{511}{881}\right)$.

3 marks per assessed part. Total for question: [15]

7. Use Gauss' Lemma to compute the following Legendre symbols:
(i) $\left(\frac{7}{11}\right)$; (ii) $\left(\frac{5}{13}\right)$; (iii) $\left(\frac{-3}{17}\right)$; (iv) $\left(\frac{5}{19}\right)$.

8*. Find all primes p such that $x^2 \equiv 13 \pmod{p}$ has a solution. **[10]**

Total for question: [10]

9. Let p be a prime with $p \equiv 3 \bmod 4$. Show that if $p \nmid a$ and the congruence $x^2 \equiv a \bmod p$ is soluble then its solution is $x \equiv \pm a^{(p+1)/4}$. Hence solve $x^2 \equiv 5 \bmod 79$.

10*. Let p be an odd prime, and put $s(a,p) = \sum_{n=1}^{p} \left(\frac{n(n+a)}{p}\right)$. Show that:

(i) $s(0,p) = p-1$. **[5]**

(ii) $\sum_{a=1}^{p} s(a,p) = 0$. **[5]**

(iii) If $(a,p) = 1$ then $s(a,p) = s(1,p)$. **[5]**

(iv) Conclude that $s(a,p) = -1$ if $(a,p) = 1$. **[5]**

Total for question: [20]